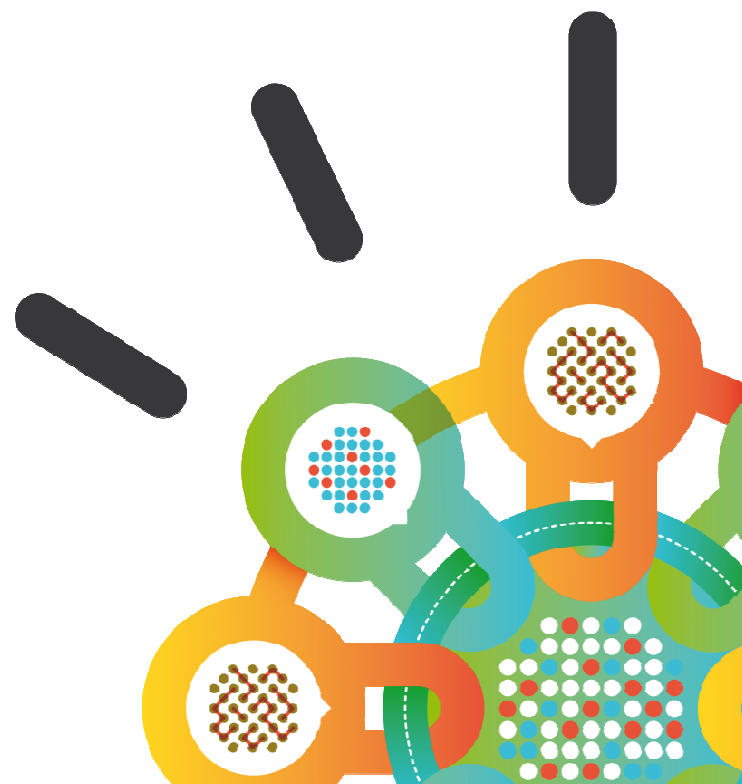


Security Intelligence.
Think Integrated.

IBM Security Systems

Security wird intelligent

Peter Häufel
IBM Security Systems
+49-175-7252260
haeufel@de.ibm.com



Problemstellung beim Kunden

- Millionen von Events nutzlos archiviert
- Kein Frühwarnsystem
- Wertvolle Daten, aber keine Information
- CSO's haben den Überblick verloren
- IT-Risikomanagement im nahezu Blindflug

Correlation is everything

Network and
User Context

Event: Attempted Privilege Gain
Target: 96.16.242.135 (vulnerable)
Host OS: Blackberry
Applications: Mail, Browser, Twitter
Location: Whitehouse, US
User ID: bobama
Full Name:Barack Obama
Department: Executive Branch

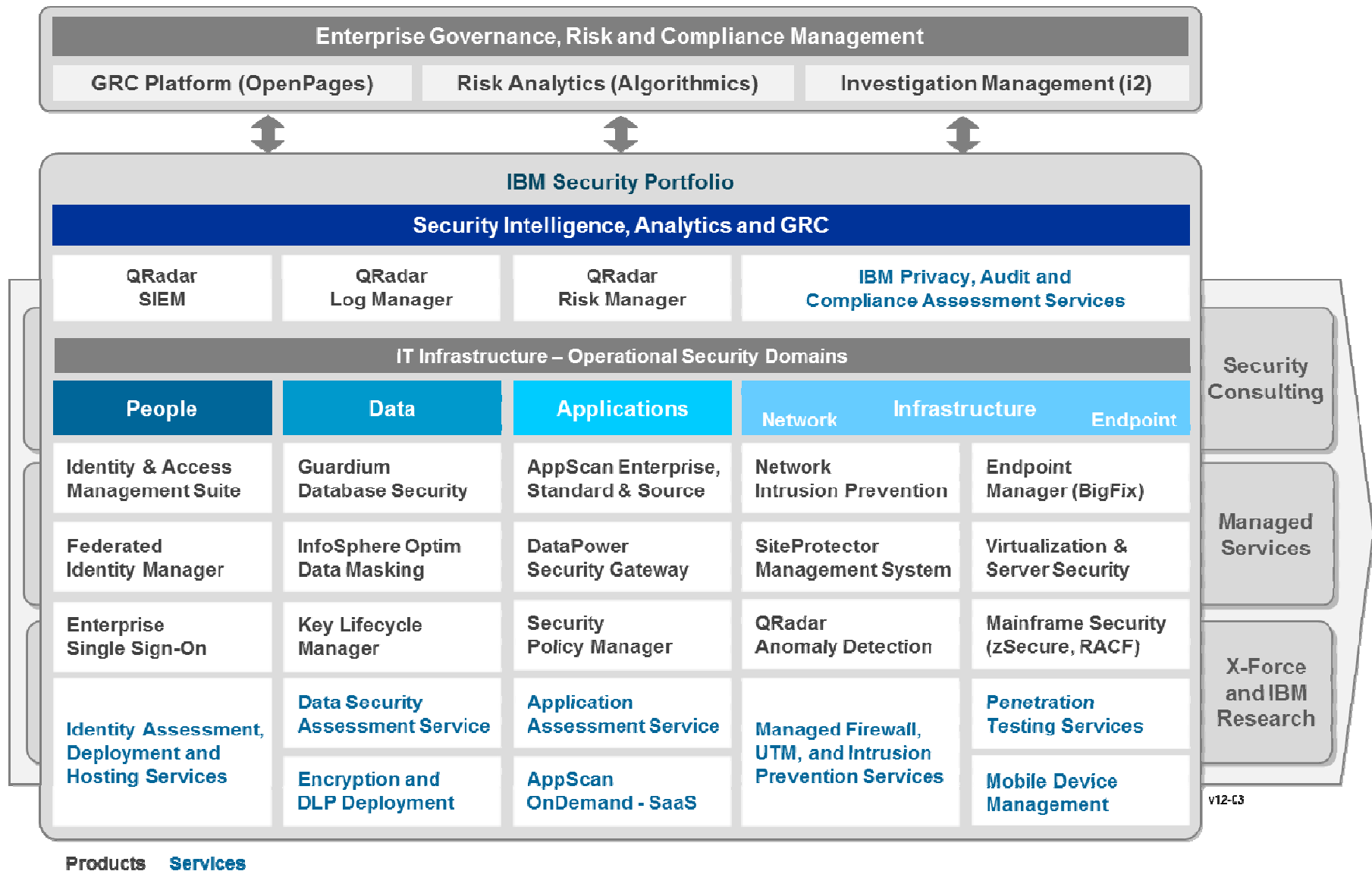
Network
Context

Event: Attempted Privilege Gain
Target: 96.16.242.135 (vulnerable)
Host OS: Blackberry
Applications: Mail, Browser, Twitter
Location: Whitehouse, US

No Context

Event: Attempted Privilege Gain
Target: 96.16.242.135

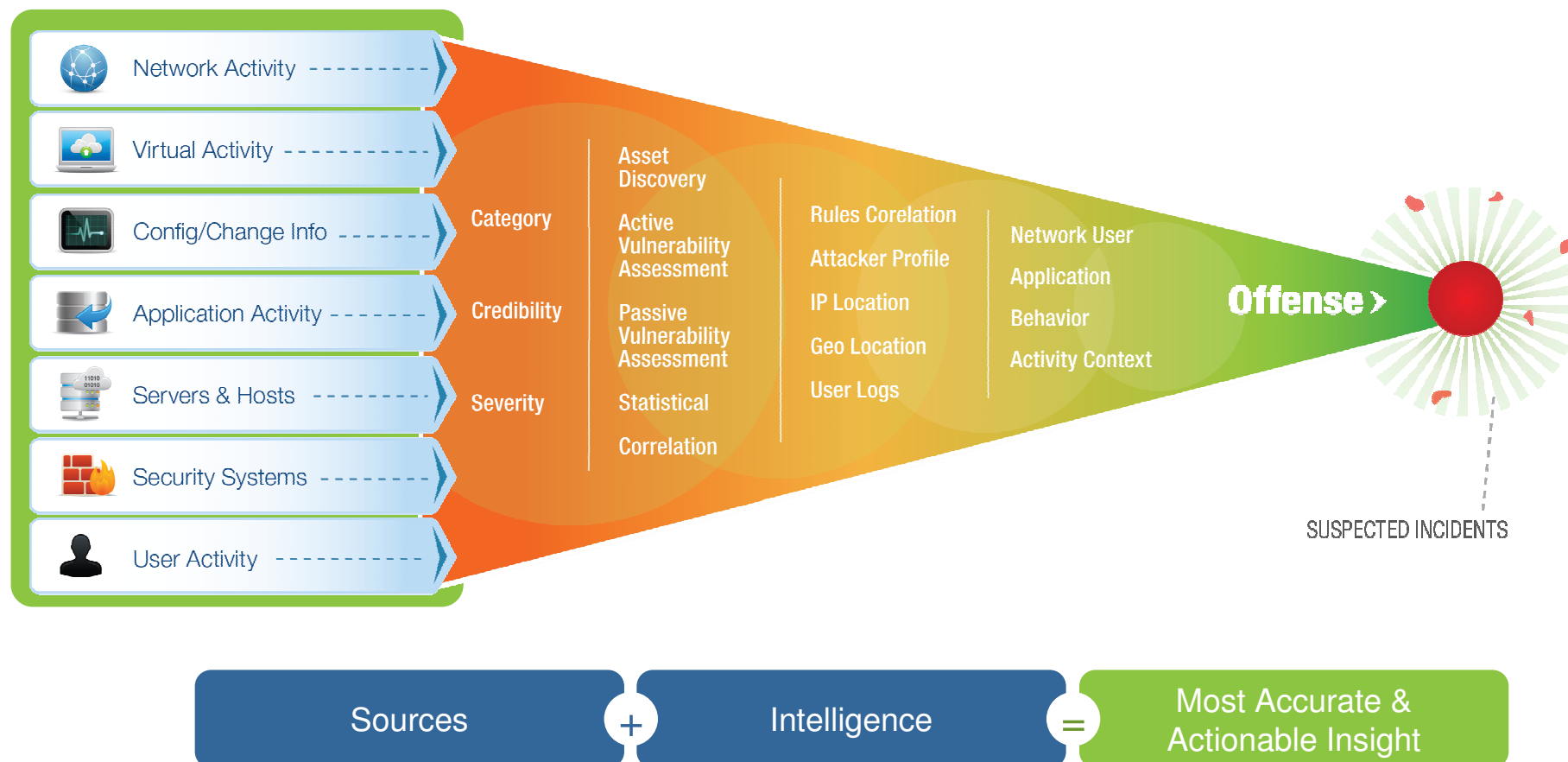
Intelligence: Leading products and services in every segment



V12-C3

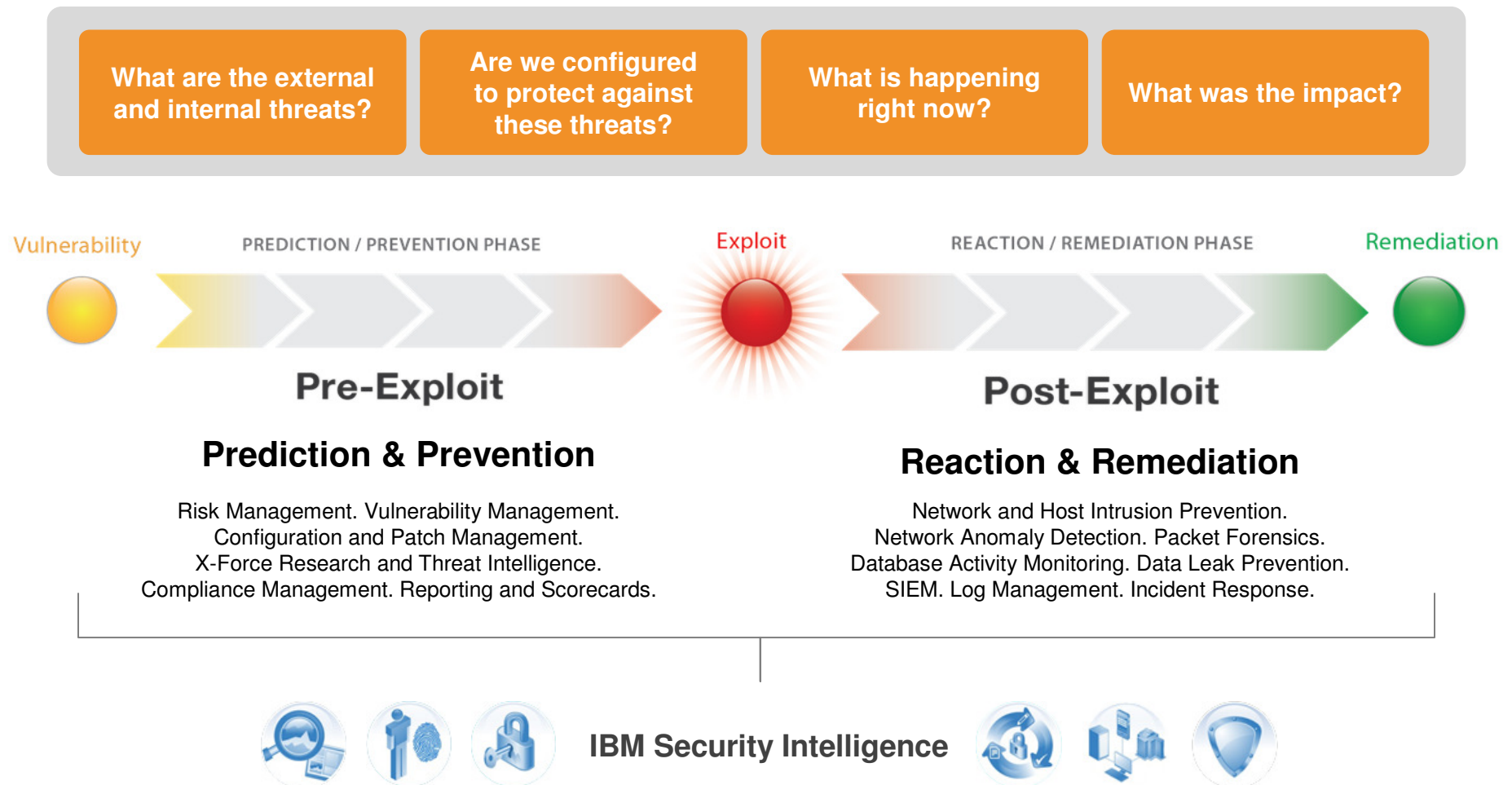
Data Explosion

IBM is integrating across IT silos with Security Intelligence solutions



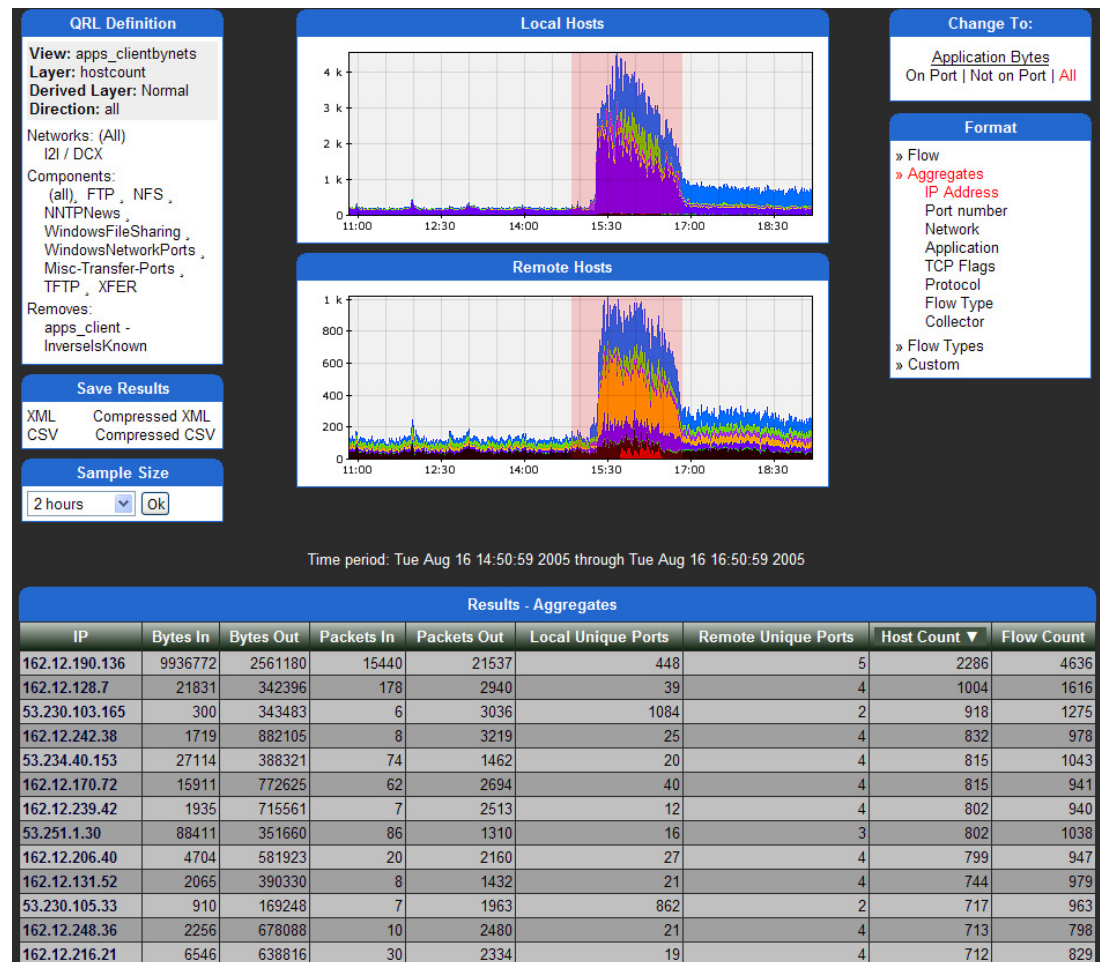
Attack Sophistication

IBM is helping clients combat advanced threats with pre- and post-exploit intelligence and action





Large Auto Manufacturer –
Detected a worm outbreak affecting their production facility during evaluation using only flow data. This worm was not detected by existing signature based sources



QRadar SIEM

Product Tour: Intelligent Offense Scoring







QRadar judges “magnitude” of offenses:

- *Credibility:*
A false positive or true positive?

- *Severity:*
Alarm level contrasted with target vulnerability

- *Relevance:*
Priority according to asset or network value

Priorities can change over time based on situational awareness

	Id	Description	Attacker/Src	Magnitude	Target (s)/Dest
	287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81		Multiple (508)
	318	Remote FTP Scanner Detected , Excessive Firewall Denies Across...	217.64.100.762		Local (99)
	274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49)		WebApp-Serv
	308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.86		Local (8)
	309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.85		Multiple (2)
	286	Remote FTP Scanner Detected , Excessive Firewall Denies Across...	81.240.89.210		Remote (226)
	296	Malware - External - Communication with BOT Control Channel ,...	10.100.100.208		Remote (2)
	236	VOIP: Pingtel Xpressa Denial of Service	10.104.143.0		Multiple (2)
	314	Local Mass Mail Host Detected	10.100.50.21		Multiple (7)
	290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.100		10.100.150.20
	291	Authentication: Repeated Login Failures Single Host , Login F...	10.100.50.64		Multiple (3)
	284	DoS - External - Flood Attack (Low)	205.174.165.5		Remote (1)

QRadar SIEM

Product Tour: Offense Management

Clear, concise and comprehensive delivery of relevant information:

Offense 3063 Summary Attackers Targets Categories Annotations Networks Events Flows Rules Actions Print ?

Magnitude				Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan			Event count	1428 events in 3 categories				
Attacker/Src	202.153.48.66			Start	2009-09-29 16:05:01				
Target(s)/Dest	Local (717)			Duration	1m 32s				
Network(s)	Multiple (3)			Assigned to	Not assigned				
Notes	Vulnerability Correlation Use Case Illustration: An attacker originating from China (202.153.48.66) is exploiting a vulnerability data with IDS alerts An attacker originating from China (202.153.48.66) is exploiting a vulnerability data with IDS alerts An attacker originating from China (202.153.48.66) is exploiting a vulnerability data with IDS alerts								

Attacker Summary Details

Magnitude	202.153.48.66		User	Karen
Description	202.153.48.66		Asset Name	Unknown
Vulnerabilities	0		MAC	Unknown
Location	China		Asset Weight	0

Top 5 Categories Categories

Name	Magnitude	Local Target Count
Buffer Overflow		8
Misc Exploit		3
Network Sweep		1417

Top 5 Local Targets Targets

IP/DNS Name	Chained	User	MAC	Location	Weight
Windows AD Server		Unknown	Unknown	main	8
10.101.3.3	Unknown	No	Unknown	main	0
10.101.3.4	Unknown	No	Unknown	main	0
DC106	Yes	No	Adn	main	10
10.101.3.11	Unknown	No	DC	main	0

Top 10 Events Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		1.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm		1.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		1.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		1.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		1.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

Annotations:

- What was the attack? (Points to Description)
- Who was responsible? (Points to Attacker Summary)
- Was it successful? (Points to Relevance/Severity/Credibility)
- Where do I find them? (Points to Top 5 Local Targets)
- How many targets involved? (Points to Top 5 Local Targets)
- How valuable are the targets to the business? (Points to Weight column in Top 5 Local Targets)
- Are any of them vulnerable? (Points to Chained column in Top 5 Local Targets)
- Where is all the evidence? (Points to Top 10 Events)

Solving complex problems that point solutions cannot



Improving threat detection

Discovered 500 hosts with “Here You Have” virus, which all other security products missed



Consolidating data silos

2 billion log and events per day reduced to 25 high priority offenses



Predicting risks against your business

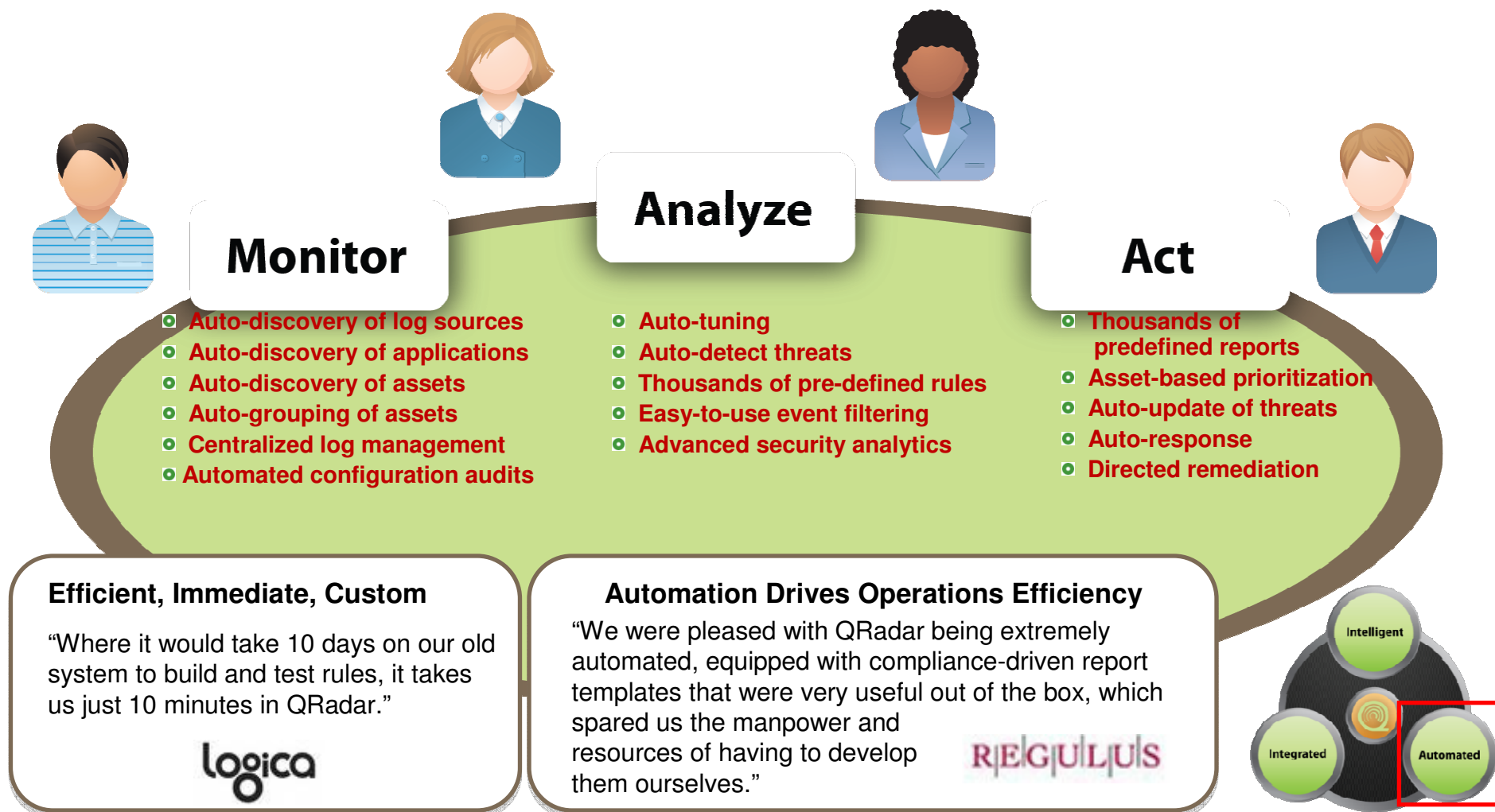
Automating the policy monitoring and evaluation process for configuration changes in the infrastructure



Addressing regulatory mandates

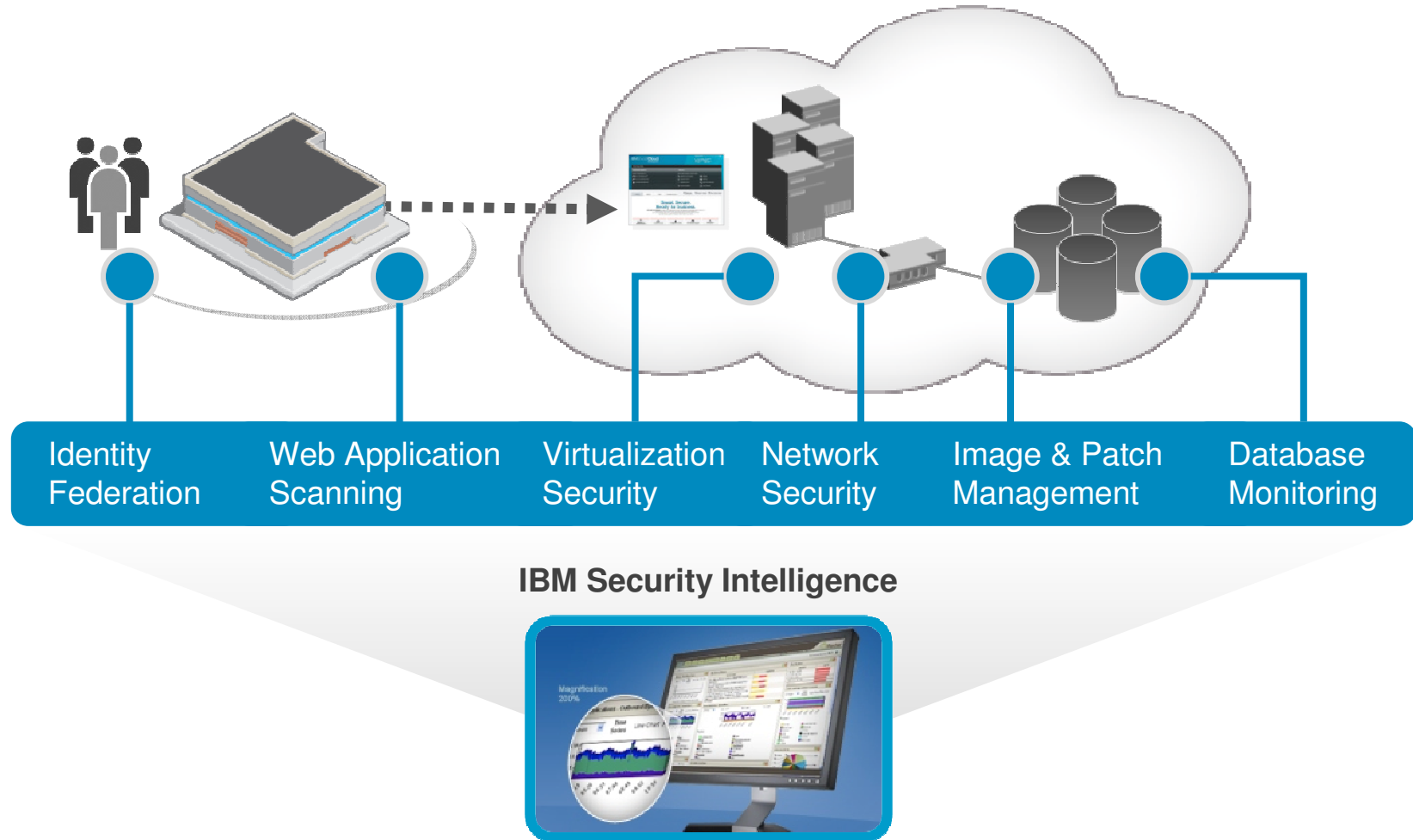
Real-time monitoring of all network activity, in addition to PCI mandates

QRadar: Automation Drives Simplicity and Cost Effectiveness



Everything is Everywhere

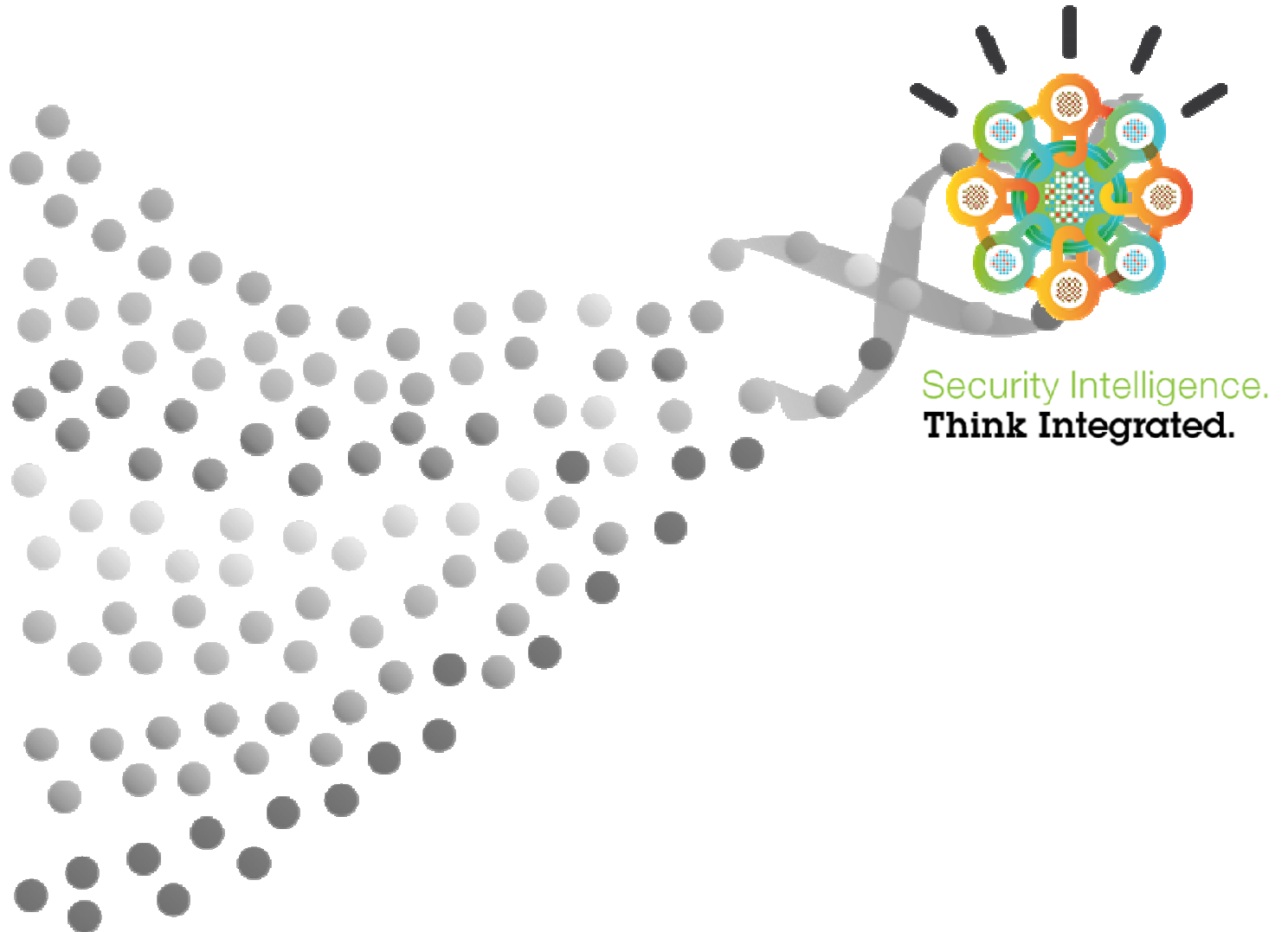
IBM is helping clients adopt cloud with flexible, layered security solutions



Positionierung

- Leading Quadranten bei Gartner
- Referenzkunden in nahezu allen Branchen
- Produkt und kein Framework
- Eine Konsole (TCO)
- Extrem skalierbar
- Vieles automatisiert – Schneller „Buy to Value“
- PoC, PoC, PoC !

Intelligent solutions provide the DNA to secure a Smarter Planet





ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.